AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN

TIPOS DE AMENAZAS

Las amenazas se pueden agrupar básicamente en cuatro categorías

- Factores humanos
- Fallas en los sistemas de procesamiento de información
- Desastres naturales
- Actos maliciosos o malintencionados

DESCRIPCIÓN DE LAS PRINCIPALES AMENAZAS

- **Spyware (programas espías)**

Es un código malicioso cuyo principal objetivo es recoger información sobre las actividades de un usuario en un computador, para permitir el despliegue sin autorización en ventanas emergentes de propaganda de mercadeo, o para robar información personal. Hay iniciativas de utilizarlos para controlar el uso de software pirata. Según las estadísticas, cerca del 91% de los computadores tienen spyware instalado, y de acuerdo a un reporte de la firma EarthLink.

- **Troyanos, Virus y gusanos**

Son programas de código malicioso, que se alojan de diferentes maneras en los computadores con el propósito de permitir el acceso no autorizado a un atacante, o permitir el control de forma remota en los sistemas. El virus adicionalmente, tiene como objetivo principal ser destructivo, dañando la información de la máquina, o

generando el consumo de recursos de manera incontrolada para bloquear o negar servicios.
El vector de propagación de estos códigos es, casi siempre, otro programa o archivo (un programa ejecutable) de otra parte, los virus, se replican ellos mismos una vez instalados en el sistema.
Las estadísticas indican que mensualmente se generan cientos de estos programas, cuyo principal objetivo es robo financiero, poniendo en riesgo la información confidencial y el dinero de las personas y de las organizaciones, más que la destrucción de archivos.
La última tendencia en clases de virus se denomina cripto-virus que una vez instalado, cifra la información contenida en el disco del equipo y posteriormente solicita una cantidad de dinero para que sus autores entreguen las claves para recuperar el contenido de los archivos cifrados (secuestro express de la información).

- **Phishing**

Es un ataque del tipo ingeniería social, cuyo objetivo principal es obtener de manera fraudulenta datos confidenciales de un usuario, especialmente financieros, aprovechando la confianza que éste tiene en los servicios tecnológicos, el desconocimiento de la forma en que operan y la oferta de servicios en algunos casos con pobres medidas de seguridad.
Actualmente, los ataques de phishing son bastante sofisticados, utilizando mensajes de correo electrónico y falsos sitios web, que suplantan perfectamente a los sitios originales.

- **Spam**

Es el recibo de mensajes no solicitados, principalmente por correo electrónico, cuyo propósito es

difundir grandes cantidades de mensajes comerciales o propagandas.
Se han presentado casos en los que los envíos se hacen a sistemas de telefonía celular – mensajes de texto –

- **Botnets (redes de robots)**

Son máquinas infectadas y controladas remotamente, que se comportan como zombis, quedando incorporadas a redes distribuidas de computadores llamadas robot, que envían de forma masiva mensajes de correo "spam" o código malicioso, con el objetivo de atacar otros sistemas; se han detectado redes más de 200.000 nodos enlazados y más de 10.000 formas diferentes de patrones de "bots".

- **Trashing**

Un método cuyo nombre hace referencia al manejo de la basura. No es una técnica relacionada directamente con los sistemas de información, pues los atacantes se valen de otra forma de ingeniería social y para ello, el mecanismo utilizado, es la búsqueda de las canecas de la basura o en los sitios donde se desechan papeles y documentos de extractos bancarios, facturas, recibos, borradores de documentos etc. Para luego utilizar esta información a conveniencia, elaborando un perfil de la víctima para robar su identidad, o teniendo acceso directamente a la información que se suponía confidencial.

ATAQUES INFORMÁTICOS

Según los datos de la encuesta anual de seguridad del FBI, los virus informáticos siguen siendo la principal fuente de perdida financiera en las organizaciones, seguidos por los impactos generados de accesos no autorizados a los sistemas, el robo de información de propiedad industrial, y la perdida de computadores personales o elementos de computación móvil. Estas causas generan más del 74% del total de las pérdidas financieras.

Según un estudio publicado por AvanteGarde , que realizo una prueba consistente en dejar unos sistemas conectados a internet con las protecciones básicas configuradas de fábrica, el tiempo promedio en el que un equipo resultó atacado fue de 4 minutos.

La falla principal que permite que los usuarios sean atacados y sean víctimas de la gran cantidad de amenazas, radica en que en muchos casos no se gestiona la tecnología dentro de un marco completo de protección de la información, y en la falta de concientización a las personas en los riesgos relacionados con el uso de la tecnología y del internet. Las inversiones en tecnología de seguridad, como solución a los problemas planteados, deben ser realizadas dentro de un marco sincronizado con otra serie de medidas para formar lo que se conoce como un sistema de gestión de la seguridad de la información.

IDENTIFICACIÓN EN LA RED

Todos los sistemas informáticos conectados en red poseen identificadores para poder enviar y recibir la información desde otros sistemas. Esta identificación se conoce como dirección IP (protocolo de internet).

Para que un sistema pueda acceder a internet, necesita tener una dirección ip única, para situaciones normales como envío de correo ofensivo, navegación , descarga de archivos, conversación con otros usuarios, es posible encontrar el rastro dejado por el computador utilizado, y en algunos casos lograr detectar la dirección física.

La red no es totalmente anónima, pero para lograr la identificación muchas veces se requiere de la colaboración de entidades como los proveedores de acceso a internet y las empresas que prestan servicio de alojamiento de páginas web.

Los sistemas informáticos utilizan niveles pobres de autenticación tanto de sistemas como de usuarios, lo cual disminuye la posibilidad de actuar contra los atacantes. Para ataques elaborados como envío de spam, virus o inclusive accesos no autorizados, los atacantes han desarrollado técnicas que permiten utilizar direcciones simuladas o falsas cambiando la dirección original asignada, y de esa forma engañan los procesos de búsqueda e identificación y en muchos casos se valen de servidores públicos, para que en caso de ser identificados, se puedan mover fácilmente a otros sistemas sin dejar rastro y así continuar con sus ataques.

LA GESTION DE LA SEGURIDAD DE LA INFORMACION

La información es un activo que, al igual que los otros activos del negocio es esencial para la organización, y por lo tanto debe ser protegido de forma adecuada.

La OCDE desarrolló por primera vez en 1992 una serie de directrices para la seguridad de los sistemas de información, las cuales tratan de promover el uso y desarrollo de una cultura de la seguridad, no solo en el desarrollo de sistemas y redes de comunicación, sino mediante la adopción de nuevas formas de pensamiento y comportamiento en el uso de la interconexión de esos sistemas.

Las directrices son:

- Concientización
- Responsabilidad
- Respuesta adecuada
- Ética
- Democracia
- Evaluación del riesgo
- Diseño y realización de la seguridad
- Gestión de seguridad
- Reevaluación

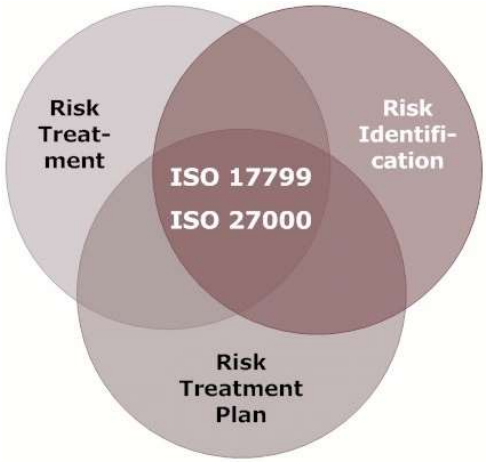
Con la evolución de los sistemas de información y de la forma de hacer negocios, la información se ha convertido en uno de los activos de mayor valor para las organizaciones. "los sistemas, redes y servicios de información afines deben ser fiables y seguros".

Los objetivos que se buscan con la gestión de la seguridad de la información son la protección de la confidencialidad, integridad y disponibilidad de la información y los bienes que la contienen o procesan. De esta manera las organizaciones se pueden proteger de:

- Divulgación indebida de la información sensible o confidencial, de forma accidental o sin autorización
- Modificación sin autorización o de forma accidental de información crítica, sin conocimiento de los propietarios
- Perdida de información importante sin posibilidad de recuperarla
- No tener acceso o disponibilidad de la información cuando se necesita

La información debe ser manejada y protegida adecuadamente de los riesgos o amenazas que enfrente, la información valiosa se puede encontrar en diferentes formas; impresa, almacenada electrónicamente, trasmitida por diferentes medios de comunicación o de transporte, divulgada por medios audiovisuales, en el conocimiento de las personas etc.

ESTANDARES ISO



Los estándares ISO 17799 e ISO 27001 dan las bases para desarrollar un marco de gestión de la seguridad de la información efectivo, que le permita proteger sus activos e información importantes, minimizando sus riesgos y optimizando las inversiones y esfuerzos necesarios para su protección.

Una de las formas de protección consiste en la aplicación de controles, que en la práctica pueden ser políticas, procesos, procedimientos, organización, elementos de hardware y software, mecanismos de protección de la infraestructura física y de seguridad, asi como la adecuada selección y entrenamiento del personal que opera y utiliza los recursos de información.

La norma ISO 17799 presenta una serie de áreas para ser gestionadas, mediante la aplicación de controles o mecanismos de protección, las cuales van desde la seguridad en los sistemas, pasando por los aspectos de seguridad física, recursos humanos y aspectos generales de la organización interna de las organizaciones.

CUMPLIMIENTO LEGAL

La norma ISO 17799 contiene un capitulo con referencias de buenas prácticas para desarrollar los controles necesarios que se deben aplicar en las organizaciones para tener en cuenta los aspectos legales y regulatorios como parte de la gestión de la seguridad de la información. Un punto importante que se debe tener en cuenta, es la protección adecuada para el uso correcto de los sistemas o recursos informáticos para evitas el uso indebido de esos recursos, de manera que puedan afectar a terceros.

Aspectos como el cumplimiento y protección de propiedad intelectual, derechos de autor, licencias de software, registros de la organización, información confidencial de clientes, empleados o proveedores, así como el cumplimiento de regulaciones provenientes de organizaciones o entes de control como la superintendencia, los ministerios, Basilea, organismos reguladores de comercio electrónico, ley "Habeas Data", son aspectos que deben ser incorporados en la definición y aplicación de mecanismos de protección de la información.

REFERENCIAS

Cesar H Tarazona, "Amenazas informáticas y seguridad de la información" recuperado de: revistas.uexternado.edu.co/index.php/derpen/article/download/965/915

Imágenes:

Imagen1, recuperada de:

https://www.computerhope.com/jargon/a/antispy.htm

Imagen 2, recuperada de:

http://www.monografias.com/trabajos77/tecnicas-ataque-seguridad/tecnicas-ataque-seguridad2.shtml

Imagen 3, recuperada de: https://www.avast.com/es-es/c-phishing

Imagen 4, recuperada de: https://es.slideshare.net/Eliascg18/el-spam-informtico

Imagen 5, recuperada de: http://www.danysoft.com/los-12-peores-botnets/

Imagen 6, recuperada de: https://pixabay.com/es/cubo-de-basura-papelera-encendedor-23640/

Imagen 7, recuperada de: https://geeksroom.com/2017/08/fbi-detiene-al-investigador-seguridad-informatica-responsable-detener-ataque-del-malware-wannacry/112353/

Imagen 8, recuperada de: https://norfipc.com/redes/cambiar-direccion-ip-dinamica-estatica.html

Imagen 9, recuperada de: https://www.youtube.com/watch?v=RNQnftdvKxA

Imagen 10, recuperada de: http://auditoriadesistemasadrimeli.blogspot.com.co/2013/09/las-iso-17779-y-27001.html

Imagen 11, recuperada de: https://www.emaze.com/@AZZOWWOC